

AccuKnox VS Sysdig

Secure Entire Ecosystem, Not Just Containers

AccuKnox offers broader coverage than Sysdig, protecting cloud, containers, Kubernetes, and more with runtime security and zero trust principles. Supports 33+ compliance frameworks for effortless regulatory adherence; users report 89% fewer false positives.



Better

AccuKnox offers superior protection across cloud, containers, and Kubernetes environments, supporting over 33 compliance frameworks and enhanced by open-source innovations like KubeArmor, trusted by over 1 million downloads.



Faster

AccuKnox speeds up security operations with real-time runtime protection, cutting remediation time by 91% and reducing false positives by 89%, making threat detection and response significantly more efficient.



Cheaper

AccuKnox delivers a unified Cloud Native Application Protection Platform (CNAPP) that lowers total cost of ownership by consolidating multiple security tools into one solution, offering flexible pricing that scales seamlessly for organizations of all sizes.

Application Security Coverage



Registry scan (ECR, GCR, Nexus, Docker Hub, ACR, Harbor, Quay, jFrog, OpenShift, GAR)



Single scanner can be used to scan multiple registries



Supports scanning public registries



Identify 3rd Party Dependencies and their Vulnerabilities (SCA), Scan for Vulnerability in Code (SAST) and Evaluate Applications for Vulnerabilities (DAST)



Integrate with CI/CD for detecting secret leakage and Shift Left Automation with Prioritization



Application Behavior Analysis - Provides deep observability by leveraging eBPF



Registry Scan (JFrog Artifactory, Amazon ECR, Docker Trusted Registry, GCR, GAR, Harbor, ACR, Quay)



A new registry scanner must be installed per registry (except for AWS Organization)



Public registries are not supported



Scans Container, IaC, Kubernetes manifest scan. Sysdig provides SAST using [integrations](#)



Allows integration with CI/CD Pipelines



Leverages eBPF for deep observability

Observability and Remediation



Auto generation of policies based on the activity discovered inside containers to prevent anything that deviates from it



Graphical view of identities in Kubernetes with customizable queries to define least permissive posture



Provides policies that harden the workloads and prevents violations before they happen



Zero day attack protection by defining the least permissive posture of the application. This will prevent any new activity that is unexpected in the application



CIS benchmarking of clusters to reduce attack surface and proactive prevention of attacks using admission controllers



Provides pre-built policies and allows customization to detect malicious activity and send alerts. Auto Tuning helps reduce false positives



Does not provide a graphical view of the entities and their relationships



Policies are reactive and kill the processes after they are found to violate the policy



Helps identify malicious activity and quick reactions to zero day attacks



Supports Admissions Controller and CIS Benchmarking of clusters

Hardening and Prevention

Deployment Models



Air-gapped and On Prem Support



Supports Air-gapped and On Prem deployments



Agent based protection and Agentless scanning support



Supports Agentless scanning in addition to agent based scanning

Open vs Proprietary



Uses KubeArmor - An open source CNCF Sandbox project



Uses Falco Open Source



Ingests findings from other open source security tools



Ingests data from Open Source tools

Integrations



Integrates with both open source and proprietary scanners in addition to SIEM, Ticketing platforms



Can integrate with both Open Source and Proprietary tools

Future Proof Security



5G Workloads and IoT/Edge Security



Provides security capabilities at the Edge



CNAPP with out of the box Kubernetes Security via Posture Management (KSPM) & Identity Management (KIEM)



Provides only the KSPM capabilities

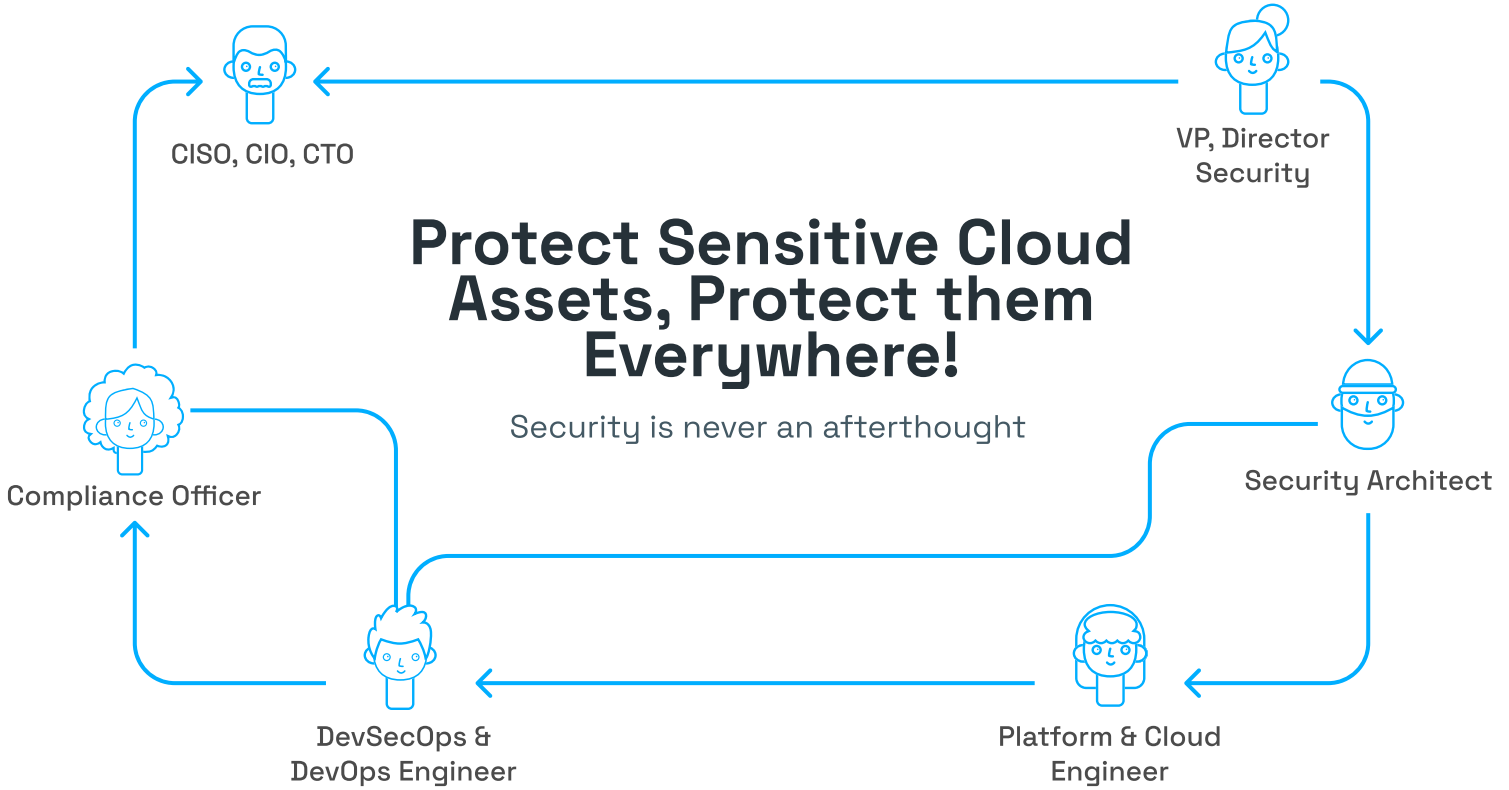


AI Security with ModelKnox (AI-SPM)



AI security is possible with AI Workload Security

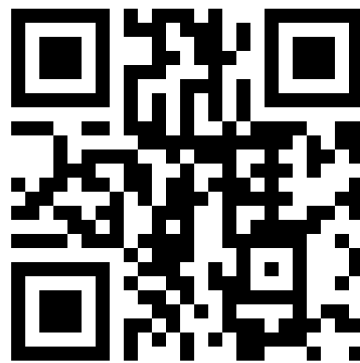
Featured by



Extra 30 Days Free Trial



*No strings attached, limited period offer!



Scan for Demo

About AccuKnox

AccuKnox is a Zero Trust CNAPP Cloud Security protects Public clouds, Private clouds, Kubernetes, VMs, Bare metals, IoT Edge, and 5G security.



in linkedin.com/accuknox

X @AccuKnox

